

PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

REC'D 29 OCT 2004

WIPO PCT

PCT / SE 2004 / 001448

Intyg Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.



(71) Sökande Solid AB, Stockholm SE
Applicant (s)

(21) Patentansökningsnummer 0302733-1
Patent application number

(86) Ingivningsdatum 2003-10-16
Date of filing

Stockholm, 2004-10-14

För Patent- och registreringsverket
For the Patent- and Registration Office


Gunilla Larsson

Avgift
Fee

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

**PATENT- OCH
REGISTRERINGSVERKET
SWEDEN**

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

LOCK SYSTEM

FIELD OF INVENTION

The present invention relates generally to lock systems
 5 and more particularly to a lock system which can be set
 up in an easy and yet secure way and be operated with a
 high security level.

BACKGROUND

Electronic or electro-mechanical lock systems having
 10 locks or the like that are connected to a central
 computer or system by means of a cable network have been
 in use for many years. The operation of these systems
 are managed from the central computer which communicate
 the applicable rules via a local network (LAN) to
 15 individual door access control (DAC) units. The DAC
 units in turn communicate e.g. log information to the
 central computer.

It is of vital importance that the communication between
 the central computer and the individual DAC units is
 20 secure, i.e., that it cannot be intercepted and
 interpreted or manipulated by a fraudulent person trying
 to gain unauthorized access to the premise in which the
 lock system is installed.

In prior art lock systems this high level of security
 25 has been achieved by the use of proprietary communi-
 cation protocols, shielded communication wires etc.
 However, today's users are not prepared to install a
 separate protected cable network for a lock system in
 parallel with a computer network already installed in

the office, such as an Ethernet based network, or to use proprietary systems tying them to one or a limited number of suppliers.

One way of achieving secure communication on a pre-existing network is to use encrypted data for communication between the central computer and the individual DAC units. However, before using encrypted communication, the different units communicating must have encryption/decryption keys installed. These keys could be installed by skilled personnel that provide each and every unit with the required keys. One problem associated with this solution is that the persons normally installing such lock systems are not skilled personnel in the sense that they are not familiar with computer hardware and software. Thus, installation of encryption/decryption keys would be performed by expensive personnel in a separate step after the physical installation of the system, leading to increased costs. Also, the use of individuals for installing software is a security risk in itself.

A problem in prior art is thus to provide a lock system which shows a high degree of security while the installation and set-up of the system can be effected in an easy way.

25 SUMMARY OF THE INVENTION

An object of the present invention is to provide a lock system wherein the prior art drawbacks are avoided and in which encryption keys can be installed in an easy and yet secure way. This means that one specific object is

that installation of components must be as simple as possible.

Another object is that security breach by customer mistakes must not affect other customers or the
5 manufacturer.

Yet another object is to provide a system and method wherein existing standards and implementations are used as much as possible.

Still yet another object is to provide a method wherein
10 system requirements are kept as small as possible.

The invention is based on the realisation that the use of certificates in combination with asymmetric and symmetric encryption in a lock system provides a secure yet efficient solution to the above described problem.

15 According to the invention there are provided method of installing a lock system as defined in claim 1 and a lock system as defined in claim 9.

By providing a lock system which is set up by means of both asymmetric and symmetric communication between the
20 units in the system both simple installation and high security are achieved.

In a particularly preferred embodiment, a unique symmetric encryption key is used for each door access control unit. This ensures that the integrity of the
25 lock system is maintained in the case one or more of the DAC units are taken over by a fraudulent person trying to gain unauthorized access to the premise in which the lock system is installed.

Further preferred embodiments are defined by the dependent claims.

BRIEF DESCRIPTION OF DRAWINGS

The invention is now described, by way of example, with
5 reference to the accompanying drawings, in which:

fig. 1 is an overall view of a the hardware including a manufacturer and customer lock systems;

fig. 2 is a block diagram showing a Public Key Infrastructure implemented in the lock system according
10 to the invention;

fig. 3 is a simplified diagram showing the different steps in the method according to the invention; and

fig. 4 is a detailed diagram showing the different steps in the method according to the invention.

15 DETAILED DESCRIPTION OF THE INVENTION

In the following a detailed description of a preferred embodiment of the present invention will be given.

In the present description, the term "lock system" is intended to cover all types of electronic lock systems
20 wherein the door access units control electronic or electro-mechanical locks, card readers, panic buttons etc. (not shown in the figures) and is thus not limited to systems comprising conventional lock cylinders or the like.

25 An environment in which the present invention is implemented will now be described with reference to figure 1. It is there shown a manufacturer computer

system 10, which comprises computer hardware with peripherals etc. and access to the Internet. The manufacturer computer system runs software adapted for processing of customer certificates. The management
5 system is divided into a front end system that collects signature request and a back end system that holds the manufacturer's private key used for signing of a customer public key. The subsystem that contain the private key responsible for signing customers'
10 certificate is not exposed to public networks .

A number of customer lock systems, generally designated 100, two of which are shown in the figure, each comprises a customer management computer 110 connected to a plurality of door access control (DAC) units 120
15 via a local area network (LAN) 130. The LAN could be Ethernet-based but the invention does not exclude other kinds of networks.

The management computer 110 is the computer wherein all rules relating to the lock system 100 is managed and
20 stored. These rules can be related to which individuals are authorised to open which doors, temporal restrictions to access to doors etc. These rules are downloaded to the individual DAC units 120 which effect the physical control of the doors by means of actuators
25 etc.

The present invention uses the well-known Public Key Infrastructure (PKI) which uses techniques for public-key encryption, also referred to as asymmetric encryption. In public-key encryption systems each entity
30 has a public key and a corresponding private key. The

public key defines an encryption transformation, while the private key defines the associated decryption transformation. Any entity wishing to send a message to another entity A obtains an authentic copy of A's public key, uses the encryption transformation to obtain the cipher text, and transmits this cipher text to A. To decrypt the cipher text, A applies the decryption transformation to obtain the original message.

The public key need not be kept secret, and, in fact, may be widely available — only its authenticity is required to guarantee that A is indeed the only party who knows the corresponding private key. A primary advantage of such systems is that providing authentic public keys is generally easier than distributing secret keys securely, as required in symmetric key systems.

Since A's encryption transformation is public knowledge, public-key encryption alone does not provide data origin authentication or data integrity. Such assurances must be provided through use of additional techniques, including message authentication codes and digital signatures. Public-key encryption schemes are typically substantially slower than symmetric-key encryption algorithms.

Public-key decryption may also provide authentication guarantees in entity authentication and authenticated key establishment protocols.

The Public Key Infrastructure in a lock system according to the invention will now be described with reference to fig. 2, wherein part of the environment shown in fig. 1 is detailed. More specifically, the manufacturer

computer system 10, a management computer 110, and a DAC unit 120 are shown therein, but not the physical interconnections (the Internet, LAN). It is here seen that the manufacturer functions as an upper level

5 Certificate Authority - CA level 1 - and the lock system owner as a lower level CA - CA level 2. To achieve a scalable installation of the DAC units 120 and to restrict problems of a comprised management computer to a customer domain, part of the PKI have been arranged as

10 this hierarchy.

The installation procedure for the lock system shown in fig. 1 will now be explained in detail with reference to fig. 3, which shows the major steps of the procedure, and fig. 4, which is a more detailed representation.

15 As a first step, the manufacturer public key is installed in the DAC unit at a trusted factory. A security feature is boot-strapped into the DAC units in the form of a certificate trusting the manufacturer's software. This means that the DAC units' software can

20 only be installed under the manufacturer's control.

Each and every DAC unit 120 is thus provided with the manufacturer public key. This is a more efficient and reliable way than providing the public key when the DAC unit already has been installed. This method also

25 provides DAC units that are essentially identical before delivery, facilitating logistics and storage.

Optionally, each DAC unit is provided with a unique serial number. However, this is not important for the present invention.

When a DAC unit boots for the first time it retrieves the installer program image, checks the signature against the factory installed manufacturer public key and starts to execute upon match. The temporary
5 installer application is capable of verifying the manufacturer's signature of the customer's public key and could verify that the certificate presented by the management computer 110 has been signed by the manufacturer computer 10. The manufacturer public
10 certificate is bundled with the installer image, which is signed by manufacturer private key.

Because the DAC units only trust the manufacturer at delivery, the customers do not have full control over their own system, which in their view is unacceptable.
15 Each customer wants control of its own system. Therefore, the customer receives a certificate signed by the manufacturer. This certificate is delivered on-line through a procedure, wherein the receiver is obliged to identify himself or herself. More specifically, the
20 receiver is indicated in the certificate as attributes. This ensures that a specific individual is responsible, increasing the security level of the inventive concept.

The certificate signed by the manufacturer is used in a further step to install a certificate trusting the
25 customer. In that way, the customer gets full control of the system except for software updating, see below.

When a lock system owner buys the management computer software and obtains media together with a unique code, the name of the lock system owner is registered in the
30 manufacturer computer 10 together with the software

version. The lock system owner is then instructed to contact the manufacturer to get its management computer public key signed by the manufacturer, i.e., the upper level CA. The lock system owner's management computer
5 public certificate is then added in a database located in the manufacturer computer 10.

When the lock system owner installs the lock system software or when the lock system 100 is about to be set up, the management computer 110 generates a symmetric
10 encryption key pair and makes available the certificate signed by the manufacturer. In that way, the management computer 110 becomes a CA of itself.

After having been connected to the LAN 130, when the DAC unit 120 is turned on, the installer program image that
15 has been installed in the DAC unit accepts the management computer public certificate signed by the manufacturer. An encrypted and authenticated channel is then established, such as by means of an SSL-session using asymmetric encryption, between the management
20 computer and the DAC unit. By means of this communication channel, the DAC unit then installs the symmetric secret key from the management computer. From this moment asymmetric methods are replaced by symmetric by terminating the asymmetrically encrypted channel and
25 establishing a symmetrically encrypted tunnel and the DAC unit could thereafter only be controlled by the management computer to prevent hostile takeover from other management computer systems.

In the preferred embodiment, the factory installed
30 manufacturer public key remains in the DAC unit to

verify software from the manufacturer. This prevents customers to remote install unauthorized software in the DAC unit.

- After the set-up of the lock system 100 has been
- 5 completed, further communications between the management computer 110 and the DAC 120 are effected by means of symmetric encryption. A unique symmetric encryption key is used for each DAC unit, i.e., the management computer uses different symmetric encryption keys for the DAC
- 10 units. This ensures that the integrity of the lock system is maintained in the case one or more of the DAC units are taken over by a fraudulent person trying to gain unauthorized access to the premise in which the lock system is installed.
- 15 Asymmetric encryption is more demanding on hardware, which is inconvenient when taking hardware costs into consideration. This is one reason why the lock system according to the invention operates in a secure yet efficient way.
- 20 It has been described how the manufacturer public key is distributed on-line. However, the manufacturer public key can also be distributed on compact disc, for example, when the software product is purchased.

- Further communication between the manufacturer and the
- 25 customer can be on-line by means of the Internet, for example, or by means of other media, such as compact disks.

In the described embodiment, the receiver of the manufacturer certificate is indicated as attributes in

the certificate. As an alternative, each certificate has a unique serial number distinguishing it from other certificates. It is also preferred that the certificate is protected by means of some kind of password, such as
5 a PIN code.

A preferred embodiment of a lock system according to the invention has been described. A person skilled in the art realises that this could be varied within the scope of the appended claims.

10 The manufacturer computer system and management computers have been described as interconnected via the Internet. It will be appreciated that some of the management computers are not connected to the outside. In that case communication between the manufacturer
15 computer system and management computers can be effected via other media, such as diskettes, compact discs etc.

For ease of understanding, the manufacturer computer system has been described as one single computer. It will be appreciated that there can be more than one
20 computer at the manufacturer having different functions.

CLAIMS

1. A method of configuring a lock system (100) owned by a lock system owner and comprising a management computer (110) connected to a plurality of door access control units (120), said method comprising the following steps:
- 5
- a) installing in the door access control units a first certificate issued by a manufacturer (10) of the lock system;
- 10
- b) providing at the management computer (110) a second certificate issued by the lock system owner and signed by the manufacturer;
- c) transmitting from the management computer to a first door access control unit of the door access units the signed second certificate together with a symmetric encryption key used by the lock system owner;
- 15
- d) installing by means of asymmetric encryption the second certificate at the first door access control unit after checking the authenticity of the signed second certificate; and
- 20
- e) establishing of symmetric encryption communication between the management computer and the first door access unit.
- 25
2. The method according to claim 1, wherein a unique symmetric encryption key is used for each door access control unit.

3. The method according to claim 1 or 2, wherein the step of installing a first certificate is performed under the control of a boot strapped security feature in the door access control unit.
- 5 4. The method according to any of claims 1-3, wherein the step of providing at the management computer a second certificate is performed on-line through a procedure, wherein a receiver identifies himself or herself.
- 10 5. The method according to claim 4, wherein the identity of the receiver is indicated in the second certificate as attributes.
6. The method according to any of claims 1-5, wherein the step of providing a second certificate
15 comprises providing a symmetric encryption key pair.
7. The method according to any of claims 1-6, wherein the step of transmitting from the management computer to a first door access control unit the signed second certificate is preformed as an SSL-session.
- 20 8. The method according to any of claims 1-7, wherein the step of installing the second certificate involves keeping the first certificate so as to verify data from the manufacturer.
9. A lock system (100) owned by a lock system owner
25 and comprising a management computer (110) connected to a plurality of door access control units (120),

characterized by

- a first certificate issued by a manufacturer (10) of the lock system provided in the door access control units (120);
- a second certificate issued by the lock system owner and signed by the manufacturer provided in the management computer (110);
- a symmetric encryption key pair provided in the management computer and a respective door access control unit (120); and
- 10 — a public asymmetric encryption key for the manufacturer provided in the door access control units.

10. The lock system according to claim 9, wherein a unique symmetric encryption key is provided for each door access control unit.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

ABSTRACT

A lock system (100) is owned by a lock system owner and comprises a management computer (110) connected to a plurality of door access control units (120). A method of configuring this system comprises the following steps: installing in the door access control units a first certificate issued by a manufacturer (10) of the lock system; providing at the management computer (110) a second certificate issued by the lock system owner and signed by the manufacturer; transmitting from the management computer to a first door access control unit of the door access units the signed second certificate together with a symmetric encryption key used by the lock system owner; installing by means of asymmetric encryption the second certificate at the first door access control unit after checking the authenticity of the signed second certificate; and establishing of symmetric encryption communication between the management computer and the first door access unit. Simple yet secure installation of the lock system is thereby achieved.

(FIG. 1)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178

1/4

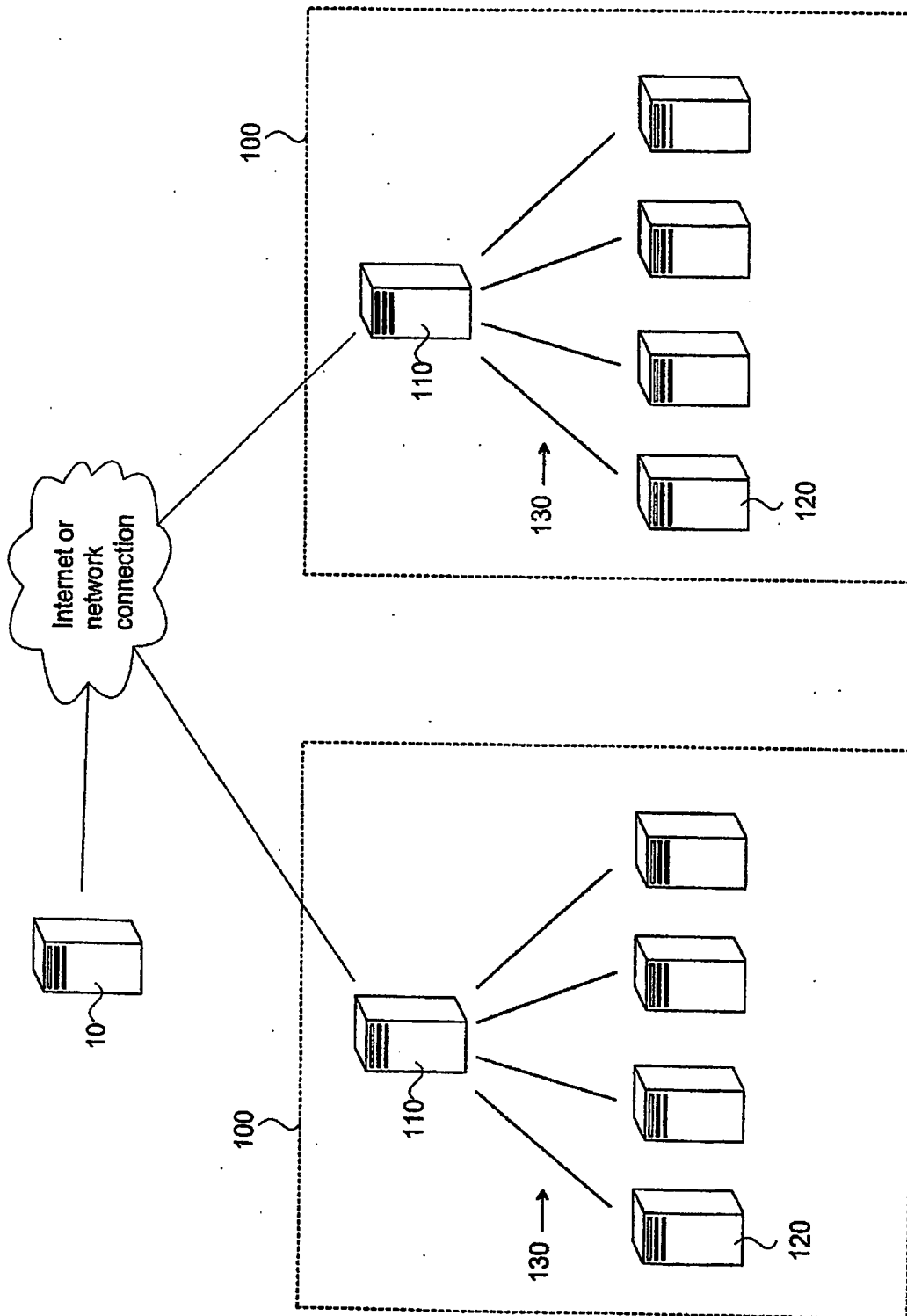


Fig. 1

2/4

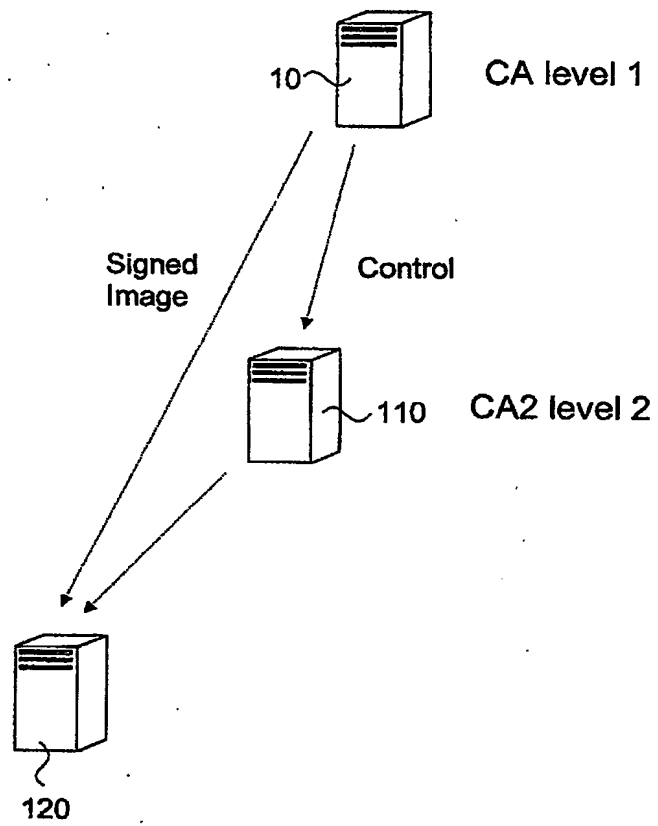


Fig. 2

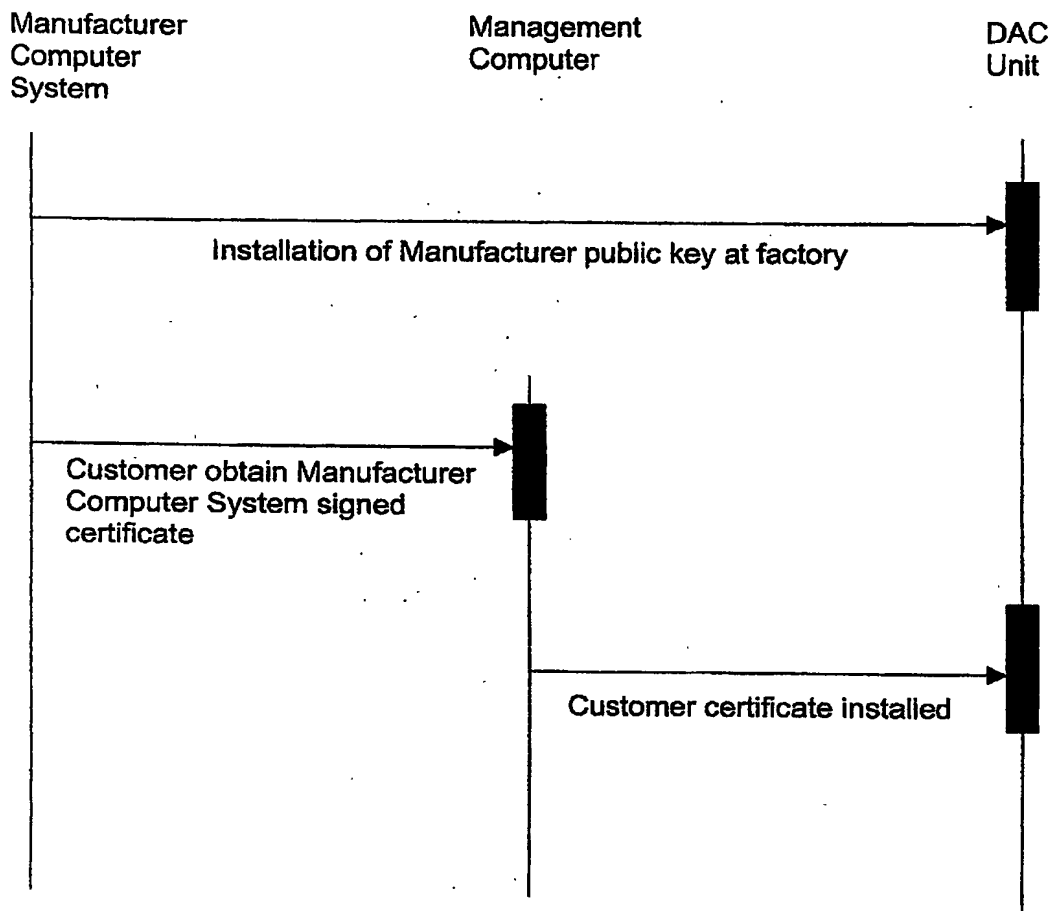


Fig. 3

1990

4/4

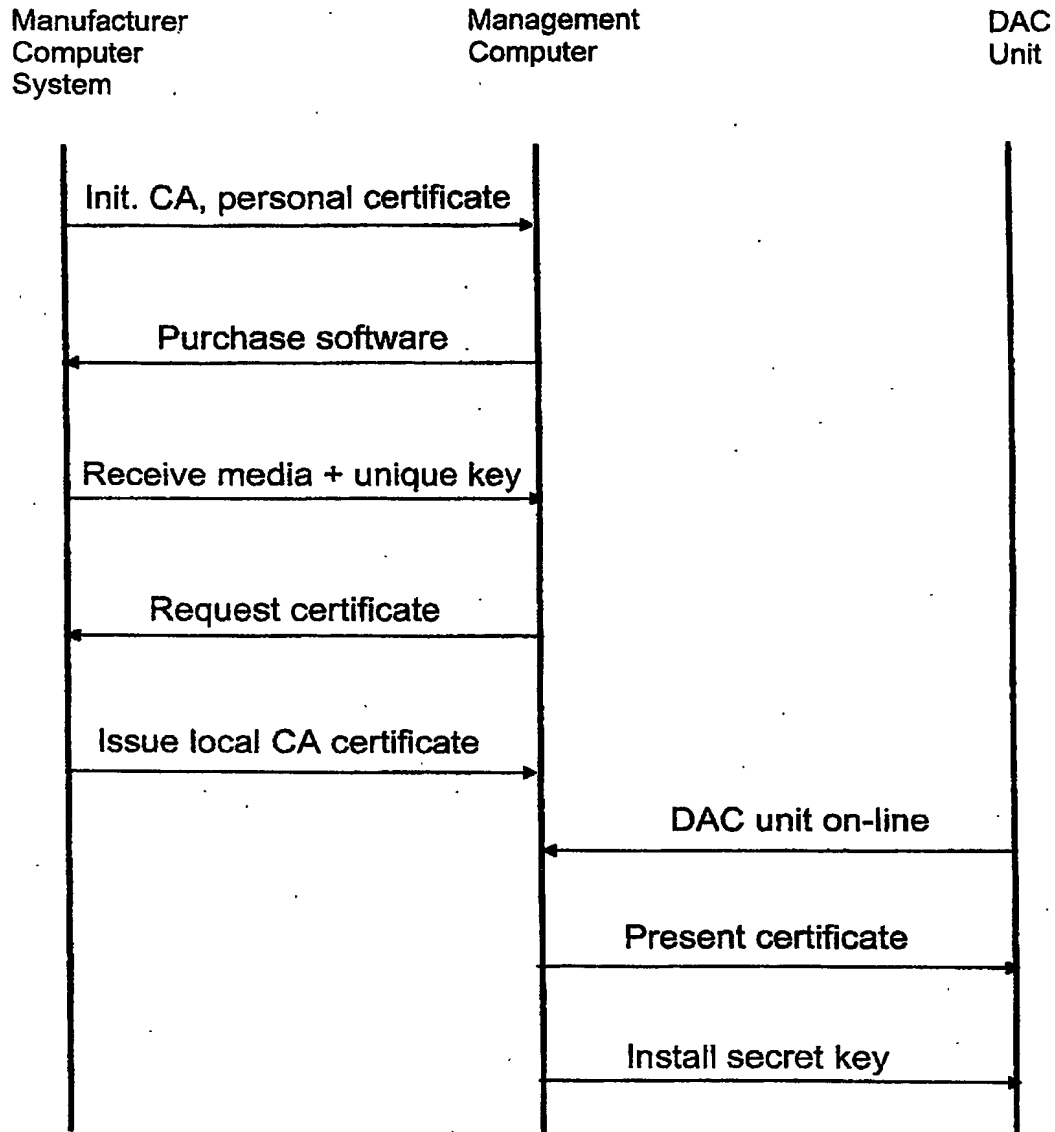


Fig. 4